REMARKS/ARGUMENTS

Applicants amend the claims to further distinguish the claims over the cited art to expedite prosecution and to correct minor errors, and canceled claim 19. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim amendments are only for facilitating expeditious prosecution. Applicants respectfully reserve the right to pursue these and other claims in one or more continuation patent applications.

The Examiner rejected claims 1-43 as anticipated (35 U.S.C. §102(e)) by Shear (U.S. Patent Pub. 2001/0042043). Applicants traverse with respect to the amended claims.

Amended claims 1, 18, and 27 concern enabling access to data in a read/write storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device, and require: providing an association of at least one coding key to the plurality of storage cartridges; encrypting the coding key; receiving an Input/Output (I/O) request; decrypting the encrypted coding key in response to the I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the at least one storage cartridges to perform the received I/O request, wherein multiple interface devices are enabled to decrypt the encrypted coding key to use to decode and code data for the storage cartridges.

The added requirement that the storage cartridges have a read/write storage medium is disclosed on at least para. [0043] on pg. 17 of the Specification. The added requirement of receiving an I/O request is disclosed on at least block 860 in FIG. 17 and para. [0057], pg. 22. The added requirement of decrypting the encrypted coding key in response to the I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the target storage cartridge to perform the received I/O request is disclosed on at least para. [0062], pgs. 24-25 and para. [0057], pg. 22 of the Specification. The added requirement that multiple interface devices are enabled to decrypt the encrypted coding key to use to decode and code data for the storage cartridges is disclosed on at least para. [0053], pg. 21 and para. [0063], pg. 25 of the Specification.

Applicants further amended claim 18 to remove the means language. With respect to claim 18, the added requirement that the I/O manager performs the operations of providing the association of keys and encrypting the coding key is disclosed on at least para. [0059] and FIG. 16 of the Specification. The added requirement that the interface device decrypts the encrypted coding key to use for the I/O request is disclosed on at least para. [0062] of the Specification.

The Examiner cited FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (Fifth Office Action, pgs. 2-3) Applicants traverse with respect to the amended claims.

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable.

Nowhere do the cited paras. 0078-0081 disclose the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the target storage cartridge to perform the received I/O request. Instead, the cited paras. 0078-0081 discuss decrypting the encrypted key block to use to decrypt content. However, there is no disclosure of decrypting a key for an I/O request to code data to be written to perform the I/O request. Further, nowhere is there any disclosure that multiple interface devices are enabled to decrypt the encrypted coding key to use to code data to write to the storage cartridges.

The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

Although the cited paras. 0127-0138 discuss how encrypted keys may be decrypted and used to decrypt content stored in a storage media, such as a DVD, nowhere does this section disclose the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to code data to be written to perform the received I/O request. Instead, the cited paras. 0127-0138 discuss how different encrypted keys may be used decrypt different content on the DVD. However, there is no disclosure of decrypting a key for an I/O request to code data to write for the I/O request. Further, nowhere is there any disclosure that multiple interface devices are enabled to decrypt the encrypted coding key to use to code data to write to the storage cartridges.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties.

Although the cited para. 0183 mentions storing protected and unprotected data on a disk, nowhere does this section disclose the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to code data to be written with respect to the storage medium of the target storage cartridge to perform the received I/O request.

The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media.

The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

In sum, all the above cited sections discuss encrypting some or all of data on a disk, such as a DVD, and then using a decryption key, which itself may be encrypted with on or more keys and stored on the disk, to use to decrypt the content on the disk. Nowhere do any of these cited sections disclose or mention the claim requirements of decrypting a key for an I/O request to code data to be written to perform the I/O request. Further, nowhere is there any disclosure that multiple interface devices are enabled to decrypt the encrypted coding key to use to code data to write to the storage cartridges.

Accordingly, for the above reasons, Applicants submit that the independent claims 1, 18, and 27 are patentable over the cited art because the cited Shear does not disclose all the claim requirements.

Claims 2-9, 19-22, and 28-35 are patentable over the cited art because they depend from one of claims 1, 18, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, the below discussed independent claims provide additional grounds of patentability over the cited art.

Applicants amended claim 22 to remove the "means" language and recite that the I/O manager transmits the encrypted coding key to the interface device. This added requirement is disclosed on at least para. [0061] of the Specification.

Amended claims 8 and 34 depend from claims 6 and 32 and further require that encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; encrypting the second key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

Applicants amended these claims to clarify the grammar and language of the claims.

The Examiner cited the above discussed sections of Shear with respect to these claims. (Fifth Office Action, pg. 4). The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that discloses encrypting the key used to decrypt the coding key with a third key, and that the interface device, or cited drive, uses a fourth key the key that is then used to decrypt the coding key, or cited encrypted key block. Further, the Examiner has not cited any part of Shear that discloses transmitting the decryption key encrypted with a first key and the second key encrypted with a third key to the interface device. In other words, the Examiner has not cited any part of Shear that discloses encrypting the key used to decrypt the coding key.

Accordingly, Applicants submit that claims 8 and 34 provide additional grounds of patentability over the cited art because the cited Shear does not disclose the additional requirements of these claims.

Amended claims 9 and 35 depend from claims 6 and 32, respectively, and further require that encrypting the coding key comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; transmitting the coding key encrypted with the first key to the interface device; receiving, from the interface device, the coding key encrypted with the first key; decrypting the coding key with the second key; encrypting the coding key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the third key to the interface device.

Applicants amended these claims to clarify the grammar and language of the claims.

The Examiner cited the above discussed sections of Shear with respect to these claims. (Fifth Office Action, pg. 5). The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key used to decrypt content on the disk with on or more keys, the Examiner has not cited any part of Shear that discloses receiving the coding key encrypted with a first key from the interface device, decrypting the coding key with a second key, reencrypting the coding key with a third key and transmitting that reencrypted coding key to the interface device, which uses a fourth key to decrypt. For instance, the Examiner has not cited any part of Shear that discloses that the DVD drive transmits the encrypted coding key to another device that decrypts that key and reencrypts with a key with a yet further key that the drive can decrypt.

Accordingly, Applicants submit that claims 9 and 35 provide additional grounds of patentability over the cited art because the cited Shear does not disclose the additional requirements of these claims.

Independent claims 10, 23, and 36 concern an interface device for accessing data in a performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, and require: receiving an encrypted coding key from a host system with an Input/Output (I/O) request; decrypting the encrypted coding key; using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request; using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

The added requirement that the storage cartridges have a read/write storage medium is disclosed on at least para. [0043] on pg. 17 of the Specification. The added requirement that an I/O request is received with the encrypted coding key is disclosed on at least blocks 770 and 860 in FIGs. 14 and17 and para. [0057], pg. 22. The added requirement of storing the received encrypted coding key is disclosed on at least para. [0058] on pg. 23.

The Examiner cited the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (Fifth Office Action, pg. 5)

Applicants submit that the Examiner has not cited any part of Shear that discloses an interface device for accessing a coupled storage medium receive an encrypted key from a host with an I/O request to decrypt and use to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD). This does not disclose decrypting the decrypted encoding key to use encode data to write to the storage medium for an I/O request.

Further, the Examiner has not cited any part of Shear that discloses the added claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. However, these cited sections do not disclose that the disk drive, which decrypted and used a key to code data to write to the storage, stores the received encrypted coding key in the storage medium for subsequent I/O requests.

Accordingly, for the above reasons, Applicants submit that the amended independent claims 10, 23, and 36 are patentable over the cited art because the cited Shear does not disclose all the claim requirements.

Claims 11-17, 24-26, and 37-43 are patentable over the cited art because they depend from claims 10, 23, and 36, which are patentable over the cited art for the reasons discussed above. Moreover, the below discussed dependent claims provide additional details grounds of patentability over the cited art.

Claims 16 and 42 depend from claims 10 and 36, respectively, and further require that the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key. These claims additionally require: receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key.

The Examiner cited the above discussed sections of Shear with respect to these claims. (Fifth Office Action, pg. 6).

Applicants submit that the Examiner has not cited any part of Shear that discloses that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear discloses that the disk drive receives a further key that is used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217 mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Accordingly, Applicants submit that claims 16 and 42 provide additional grounds of patentability over the cited art because the cited Shear does not disclose the additional requirements of these claims.

Claims 17 and 43 also provide additional grounds of patentability over the cited art for the reasons discussed with respect to claims 16 and 42 because they concern the use of third and fourth keys to encrypt and decrypt a second key that may be used to decrypt the coding key that is used to encode and code data.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-18 and 20-43 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: June 23, 2007

By: /David Victor/

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984